UNIVERSIDADE FEDERAL DO PARANÁ

ESTEVÃO SANTOS MOREIRA VANZO

ESTUDO SOBRE BITCOIN E BLOCKCHAIN E SUAS IMPLICAÇÕES

CURITIBA
2017

ESTEVÃO SANTOS MOREIRA VANZO

ESTUDO SOBRE BITCOIN E BLOCKCHAIN E SUAS IMPLICAÇÕES

Monografia apresentada como requesito obrigatório à obtenção do título de Bacharel, Curso de Ciências Econômicas, Setor de Ciências Sociais Aplicadas, Universidade Federal o Paraná.

Orientador: Prof. Walter Tadahiro Shima

CURITIBA
2017

RESUMO

O presente trabalho refere-se ao estudo da moeda digital descentralizada Bitcoin e a tecnologia que permite a sua utilização, o Blockchain. A Bitcoin é um tipo de criptomoeda, ou moeda virtual, criado no ano de 2009. Diferentemente das moedas convencionais, o bitcoin não possui um Banco Central controlando a sua valorização e desvalorização, que seguem os rumos do mercado – na lei da oferta e da procura – e as ondas de investimentos e notícias sobre o seu valor especulativo. Neste trabalho busca-se compreender o funcionamento da Bitcoin e identificar se a moeda tem potencial para causar disrupção de mercado, no sentido de alterar os agentes econômicos vigentes no sistema monetário (Banco Central e bancos comerciais) e de ameaçar a estabilidade das moedas nacionais centralizadas. A respeito da tecnologia Blockchain, procura-se entender seu funcionamento e especular sobre as possibilidades de aplicação dessa inovação em um futuro próximo.

Palavras-chave: Bitcoin. Blockchain. Criptmoeda. Tecnologia.

ABSTRACT

The present work refers to the study of Bitcoin decentralized digital currency and the technology that allows its use, Blockchain. Bitcoin is a type of criptocurrency, or virtual currency, created in 2009. Unlike conventional currencies, bitcoin does not have a Central Bank controlling its valuation and devaluation, which follow the market's directions - in the law of supply and demand - and investment waves and news about its speculative value. The purpose of this paper is to understand the functioning of Bitcoin and to identify if the currency has the potential to cause market disruption in order to change the economic agents in the monetary system (Central Bank and commercial banks) and to threaten the stability of centralized national currencies. With regard to Blockchain technology, it seeks to understand its operation and speculate on the possibilities of applying this innovation in the near future.

Keywords: Bitcoin. Blockchain. Criptocurrency. Technology.

SUMÁRIO

INTRODUÇÃO

O projeto inicial da bitcoin permitiu o surgimento da tecnologia blockchain, outras criptomoedas e novos bancos de dados virtualmente dispersos ao redor do mundo, o que remete aos bancos tradicionais se movimentarem aprofundando-se em desenvolver a blockchain, assim como as startups, financeiras e aos demais setores interessados em transações mais eficientes envolvendo um menor custo. Nesse sentido, muito se têm falado sobre a nova revolução tecnológica e assim, esse estudo procura investigar a capacidade disruptiva do blockchain e entender quais os principais agentes envolvidos no caso específico do bitcoin.

Inicialmente, criou-se a tecnologia blockchain para garantir o uso do bitcoin, que consiste no livro-razão das transações realizadas com a moeda bitcoin, anotando os saldos e transações desde a primeira operação realizada, tecnologia essa percebida como a principal inovação do bitcoin, ao comprovar todas as transações na rede. Dessa forma, procura-se analisar a importância da tecnologia blockchain e do software bitcoin no mercado e para o indivíduo, contemplando os principais requisitos de segurança na rede e as possibilidades de se aplicar o blockchain no futuro próximo.

Dessa forma, esse estudo justifica-se pela necessidade de identificar, conforme as concepções de Schumpeter se o bitcoin se mostra como uma onda perene de destruição criativa, onde a inovação varre o velho, iniciativa essa do livre mercado que movimenta o sistema capitalista, aproximando a sociedade ao eliminar os possíveis intermediários nas transações, cessando a emissão desenfreada de moeda pelos bancos centrais de países diversos. A exposição dos motivos inspiraram-se na necessidade de compreender o funcionamento do sistema comercial e financeiro na era da tecnologia digital.

Como problema de pesquisa procura-se identificar se a moeda bitcoin trata-se de uma inovação disruptiva podendo alterar os "players" vigentes no sistema monetário (os bancos e os bancos centrais) ou se trata-se somente de mais um ativo financeiro de cunho especulativo (uma nova bolha financeira).

Esse estudo tem como objetivo geral investigar o caráter disruptivo da moeda virtual no sistema capitalista, principalmente no sentido de substituir as moedas nacionais centralizadas.

1 CONTEXTUALIZAÇÃO DA MOEDA NA ECONOMIA PÓS-MODERNA

Segundo o coinBR.netblockchainTech (2017), por algum tempo o ouro foi considerado o ativo financeiro mais em evidencia, pelas suas características intrínsecas e perdura ainda nos dias atuais. Na pós-industrialização as entidades governamentais percebem que imprimir seu próprio dinheiro é um método mais conveniente para distribuir a riqueza na sociedade, embora sofra mutações pela evolução da sociedade e da própria tecnologia. (COINBR.NETBLOCKCHAINTECH, 2017).

O papel moeda não resistiu ao tempo, presenciando o fracasso de seu próprio valor monetário frente a inflação na economia, conforme registra a recente história brasileira, antes mesmo de real surgir o real, em 1994, quando então diversas moedas derrocaram na escalada da economia, como: cruzeiro, cruzado e cruzado novo.

Um estudo desenvolvido pelo DollarDaze.org (2016) mostra que tendo como base 775 moedas, não há precedente histórico de que uma moeda ao reter seu valor, pelo menos 20% delas tenham sucesso, antes, fracassaram, pela hiperinflação, 21% foram destruídas pelas guerras, 12% foram destruídas pelos movimentos de independência, 24% delas foram monetariamente reformadas e 23% estão em circulação, contudo, há fortes indícios de trilharem caminho similar de moedas mal sucedidas. Historicamente, a vida média de uma moeda tenha sido de apenas 27 anos. (COINBR.NETBLOCKCHAINTECH, 2017).

A libra esterlina, criada em 1694, no Reino Unido, se caracteriza como a mais velha moeda em existência no mundo, aos seus 322 anos, é considerada uma moeda de sucesso, desde seu surgimento seu valor foi definido ao padrão de unidade por 12 onças em prata. Em valores atuais, equivale 1/200 ou 0,5% de seu valor original, denotando em embora considerada a moeda de maior sucesso no mundo, mesmo assim, perdeu 99,5% de seu valor em sua trajetória de existência.

Em pleno século XXI existe um contingente de aparelhos celulares conectados entre os habitantes da terra, levando a crer na existência de uma moeda global, o bitcoin, que pretende fazer essa conexão entre esse contingente e assim tornar-se uma moeda digital universal, que funcione a partir de qualquer computador ou dispositivo móvel conectado à Internet (ULRICH, 2014).

Para Ulrich (2014), é analisando o contexto em que o Bitcoin surgiu que podemos compreender sua razão de ser. Foi após a crise financeira de 2008, uma das maiores crises econômicas ja observadas, que nasceu a moeda digital. Junto a isso, o avanço do estado interventor e das medidas arbitrárias das autoridades monetárias a partir do início do século XXI e a redução na privacidade no meio digital que as pessoas tem enfrentado tanto em países desenvolvidos quanto em países em desenvolvimento.

Ainda que não haja consenso para a causa da crise de 2008, pode-se dizer que o excesso de desregulamentação do setor financeiro foi fator fundamental para que ela ocorresse. De acordo com um dos tópicos de estudo da escola austríaca de economia, os ciclos econômicos são consequência inevitável das intervenções monetárias no mercado. O atual arranjo monetário do ocidente, segundo Ulrich (2014) baseia-se em dois grandes pilares. 1: O monopólio da emissão de moeda com leis de curso legal forçado. 2: um banco central responsável por organizar e controlar o sistema bancário. A interferência governamental no sistema monetário é clara, o que torna esse arranjo uma antítese do livre mercado. (ULRICH, 2014).

Além disso, as moedas hoje emitidas pelos governos não tem lastro algum, a não ser a confiança nos governos. Com o passar dos anos, o arranjo monetário foi se alterando de modo que hoje não há mais nenhum vínculo ao ouro ou a prata. O padrão ouro deixou de existir pois impunha restrições aos governos no seu ímpeto inflacionista. Quando os governos emitiam papel moeda demais, ocorria a fuga de ouro das fronteiras nacionais. Assim, eram obrigados a depreciar o câmbio com o metal precioso. (ULRICH, 2014).

Com a suspensão da conversibilidade dólar ouro em 1971, pelo presidente dos Estados Unidos da época Richard Nixon, passamos a viver na era do papel-moeda fiduciário. Nesse novo arranjo, os bancos centrais têm autonomia para imprimir quantidades quase que ilimitadas de dinheiro, com o único risco de que os cidadãos percam a confiança na moeda e parem de utilizá-la. Acontece que os governos sempre utilizaram desse artifício para financiar seus déficits, custear guerras ou suprir um estado incapaz de se manter com os impostos cobrados da sociedade. Atualmente, porém, o processo inflacionário é mais indireto e não envolve somente os Bancos Centrais, mas também todo o sistema bancário. (ULRICH, 2014).

Cédulas monetárias e depósitos bancários formam a oferta de moeda na economia. E quanto maior for a oferta monetária, menor é o poder de compra de cada

unidade monetária. Conforme Ulrich (2014), uma vez que os depósitos bancários se multiplicam por meio de um mecanismo de reservas fracionárias, é dado aos bancos o poder de criar depósitos bancários através da expansão de crédito. Desse modo, pode-se dizer que os bancos são capazes de criar moedas de fato. Mas aumentar a oferta monetária não é o único efeito da expansão de crédito. Junto a isso, surge também, a formação de ciclos econômicos. Isso acontece por não haver recursos suficientes para que os investimentos sejam completados lucrativamente, o que origina o momento de recessão. E o pior, a forma que os governos encontram de solucionar o problema é adotando a mesma medida que causou o problema. Ou seja, aumentando ainda mais a oferta monetária. (ULRICH, 2014).

Para as pessoas comuns, resta assistir o poder de compra da moeda diminuir, enquanto os bancos centrais fazem de tudo para salvar governos quebrados após o período de recessão. Tal fato deixa claro que o cidadão não tem controle algum sobre seu dinheiro. Aliado ao grande poder em suas mãos, há o fato de que os bancos centrais nem sempre são transparentes em sua atuação. Para Ulrich (2014), isso é uma grande ironia pois enquanto as autoridades monetárias se esquivam do escrutínio público, exigem cada vez mais informações da sociedade, invalidando a privacidade financeira dos cidadãos. Fato este que nos traz a outro desdobramento do paradigma atual que vivemos: a crescente perda de privacidade financeira. (ULRICH, 2014).

Com a desculpa de estar impedindo as atividades terroristas e a lavagem de dinheiro, as autoridades governamentais, principalmente dos EUA no novo milênio, tem infringido a privacidade de seus cidadãos. Através de uma lei aprovada pelo congresso em 2010, a FATCA (Foreign Account Tax Compliance), a Receita Federal dos Estados Unidos passou a ter o direito de violar o direito de privacidade de cidadãos que tenham investimentos em conta no exterior. Para Ulrich (2014, p. 41):

> Este é o paradigma do atual milênio: crescente perda de privacidade financeira; autoridades monetárias centralizadas e opressivas que abusam do dinheiro isentas de qualquer responsabilidade; e bancos cúmplices e coadjuvantes no desvario monetário. Entretanto, se por um lado o cenário é desalentador, por outro, o terreno é fértil para a busca de novas soluções. Coincidência ou não, um mês após a quebra do Lehman Brothers, era lançada a pedra fundamental de uma possível solução à instabilidade do sistema financeiro mundial.

2 CONCEITO DE BITCOIN E ANÁLISE DE SUA ESTRUTURA

O bitcoin é um software que reúne um conjunto de regras e fórmulas governadas por uma rede autônoma, desse sistema nasceu a tecnologia blockchain, que permite o funcionamento eficiente do software. O bitcoin é uma moeda similar às demais, funciona na modalidade integralmente digital, possui um sistema descentralizado, autônomo e matematizado, sem que seja necessário ser aprovado por alguma instituição intermediária para que as transações ocorram. As transações acontecem par a par (peer to peer/ponto a ponto), sendo os pagamentos realizados em dinheiro eletrônico diretamente entre as partes (HILEMAN e RAUCHS, 2017).

A bitcoin entrou em circulação em 03 de janeiro de 2009, quando Satoshi Nakamoto, pseudônimo de um usuário ainda desconhecido, publicou o protocolo e o programa que deu início ao sistema, gerando o primeiro lote de moedas. A bitcoin é uma moeda de caráter virtual e descentralizado, criada através de um programa de computador de código aberto. Desse modo, qualquer pessoa pode acessar o conteúdo de seu funcionamento e ajudar no seu desenvolvimento. É um sistema independente de qualquer agente intermediário, seja o governo ou instituições financeiras. As transações ocorrem através de uma rede peer-to-peer, cuja principal característica é a de possibilitar a troca direta de dados entre os usuários, sem a necessidade de haver um servidor central. São transferências financeiras inteiramente digitais, onde uma determinada quantidade de informação digital é transferida de um usuário para outro, com uma autorização codificada do remetente, o que faz com que as bitcoins mudem de proprietário de maneira irreversível. Além disso, todo o o processo pode ser verificado na rede, uma vez que a quantidade de moeda transacionada é informação de acesso público. Para garantir a segurança em seu funcionamento, o sistema utiliza a criptografia para codificar as informações enviadas de modo que apenas o destinatário consiga decodificá-la, o que dificulta a interceptação de uma terceira parte mal intencionada. A maior vantagem é que o usuário não estará fazendo uso de uma moeda emitida pelo governo central, é uma moeda revolucionária: dinheiro 100% digital para vidas que se tornaram a cada dia mais digitais. (COINBR.NETBLOCKCHAINTECH, 2017, NAKAMOTO, 2008, ULRICH 2014, ALI et al, 2014).

Ao falar sobre o bitcoin, para Ulrich (2014, p. 15) essa: “[...] tecnologia é tão inovadora, abarca tantos conceitos de distintos campos do conhecimento humano –

e, além disso, rompe com inúmeros paradigmas [...]". Nota-se que a capitalização total de mercado do bitcoin aumentou mais de três vezes desde início de 2016, chegando a US $ 25 bilhões em março de 2017.

Segundo Larry Summers, ex funcionário do Tesouro dos EUA: o bitcoin tem propriedade similar à máquina de fax, mas somente uma máquina de fax não teria serventia, ao passo que se todos se dispuserem do fax o instrumento se transforma em algo extremamente valioso. (BLOCKGEEKS ,2016).

No universo bitcoin, um algoritmo matemático substitui as funções de governo na emissão de moeda, sendo assim, diariamente, novos indivíduos, na política e no mundo dos negócios, dirigem sua atenção para a nova tecnologia, resultando em mudanças radicais em relação ao "dinheiro" (COINBR.NETBLOCKCHAINTECH, 2017). Nesse mesmo sentido, segundo Hileman e Rauchs (2017, p. 15):

> Bitcoin began operating in January 2009 and is the first decentralised cryptocurrency, with the second cryptocurrency, Namecoin, not emerging until more than two years later in April 2011. Today, there are hundreds of cryptocurrencies with market value that are being traded, and thousands of cryptocurrencies that have existed at some point. The common element of these different cryptocurrency systems is the public ledger ('blockchain') that is shared between network participants and the use of native tokens to incentivize participants for running the network in the absence of a central authority.

No entanto, existem diferenças significativas entre algumas criptomoedas, no que diz respeito ao nível de inovação apresentado por elas. As criptomoedas são, em sua maioria, clones do bitcoin e simplesmente apresentam valores diferentes dos parâmetros (por exemplo, tempo de bloqueio diferente, oferta de moeda, e esquema de emissão). Essas criptomoedas contribuem pouco para a inovação e são chamadas de "altcoins". Os exemplos incluem Dogecoin e Ethereum Classic.

Em contraste, surgiram novas criptomoedas que emprestaram conceitos do bitcoin, fornecendo recursos inovadores e diferenciais substantivos. Estes podem permitir a introdução de novos mecanismos de validação de transações, bem como plataformas computacionais descentralizadas com capacidades para manter "contratos inteligentes" que proporcionam funcionalidades substancialmente diferentes do bitcoin e permitem casos de uso não monetário da tecnologia. Essas novas criptomoedas e inovações do blockchain podem ser agrupadas em duas categorias: **novos sistemas blockchain** que apresentam sua própria blockchain (por exemplo, Ethereum, Peercoin, Zcash) e **dApps/outros** sistemas que existem em

camadas adicionais construídas em cima de um blockchain já existente (Counterparty, Augur). (HILEMAN e RAUCHS, 2017).

A capitalização de mercado combinada de todas as criptomoedas aumentou mais de três vezes desde o início de 2016, atingindo cerca de US $ 27 bilhões em abril de 2017. Uma pequena parcela de valor, mas não insignificante, é alocada para as “cópias” (ou seja, altcoins), enquanto uma parcela crescente tem sido compartilhada com criptomoedas inovadoras (novas criptomoedas e inovações no blockchain). (HILEMAN e RAUCHS, 2017).

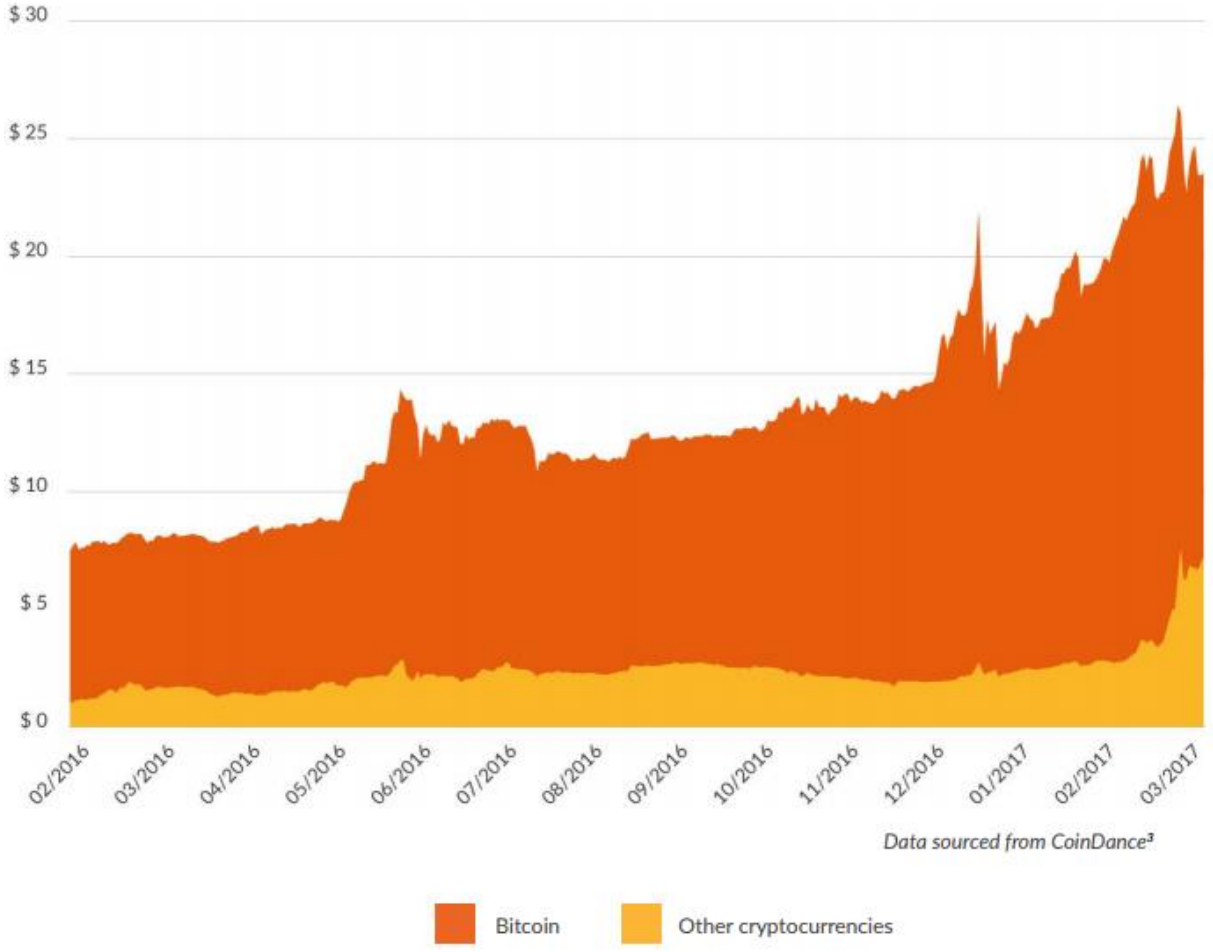

GRÁFICO 1: Capitalização do Mercado Criptigráfico (2016-2017)
FONTE: Hileman e Rauchs (2017, p. 16).

No entanto, a Bitcoin continua a ser o líder claro, tanto em termos de capitalização de mercado quanto termos de uso, apesar do aumento do interesse em outras criptomoedas. Bitcoin também é a criptomoeda que é suportada e usada pela esmagadora maioria das carteiras, trocas e provedores de serviços de pagamento, como pode ser observado no Gráfico 2.

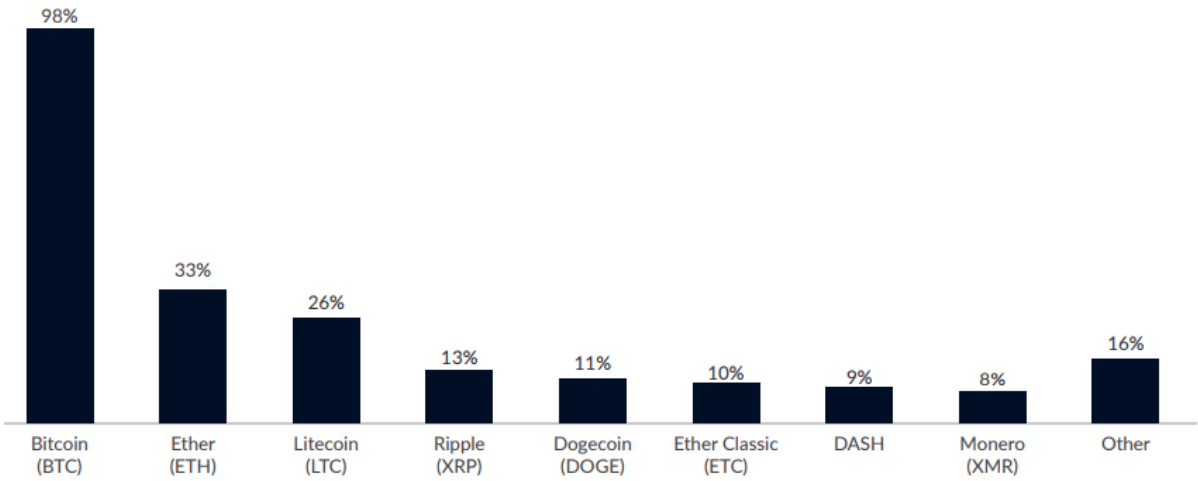

GRÁFICO 2: Grau de Utilização das Criptomoedas
FONTE: Hileman e Rauchs (2017, p. 16).

2.1 Funcionamento do Sistema Transacional

Segundo coinBR.netblockchainTech (2017), a moeda virtual bitcoin permite que duas pessoas, ainda que sejam desconhecidas, realizem suas transações comerciais e financeiras com segurança, utilizando a rede global virtual de trocas, constituída pela diversidade de pessoas que por anos consecutivos pesquisaram uma tecnologia computacional que tornasse possível essas nova realidade virtual. O fato é que simplificou as relações comerciais e negociais entre sujeitos geograficamente distantes pelo simples manuseio do telefone celular, o que permite duas pessoas transacionar comercialmente, não dependendo mais de uma autoridade central, companhia ou banco intermediário no processo, funcionando de maneira segura, transparente e incontestável. (COINBR.NETBLOCKCHAINTECH, 2017).

O funcionamento do bitcoin, sob o ponto de vista técnico, é complicado e exige conhecimentos em informática. Desse modo, buscarei apresentar neste trabalho uma descrição das etapas que envolvem a aquisição e a transferência de bitcoins, para a compreensão dos aspectos econômicos da moeda virtual.

Quando se fala em sistemas de pagamentos eletrônicos, surge um problema chamado de gasto duplo. O gasto duplo é um problema que ocorre quando um usuário utiliza mais de uma vez o mesmo dinheiro digital. Por exemplo, o usuário A transfere uma unidade de dinheiro virtual para B, porém essa quantia (por alguma falha no sistema) não sai de seu registro próprio, o que permite que esse dinheiro seja novamente utilizado. No caso do bitcoin, porém, o registro histórico é distribuído a

todos os usuários instantaneamente através da rede peer-to-peer, o que faz com que o problema do gasto duplo seja impossível de ocorrer. Assim, em vez de o registro histórico ser distribuído a um intermediário, todos os usuários mantém o registro público das transações. Isto é chamado blockchain, um banco de dados com todas as transações que alcançaram consenso dos usuários. (ALI et al, 2014).

Para explicar o funcionamento do bitcoin, serão apresentados os meios de adquirir bitcoins e suas etapas. Existem duas maneiras de se comprar bitcoins: direto de uma pessoa física, ou de uma exchange que tenha bitcoins a venda. Exchanges são empresas que fazem a ligação entre vendedores e compradores. Os vendedores podem colocar suas bitcoins a venda pelo preço desejado e os compradores podem aceitar o preço de venda ou podem lançar ordens de compra num determinado preço desejado, o que dará origem a um livro de ofertas como observado na Figura 1.

FIGURA 1: Livro de ofertas.
FONTE: https://foxbit.exchange/#offerbook. (2017).

Primeiramente, é necessário um cadastro no site da exchange, enviando cópia do documento de identificação e cópia do comprovante de residência, para poder depositar valores em dinheiro. Uma vez cadastrado, o usuário estará habilitado para

fazer depósitos no site. Os depósitos poderão ser em dinheiro, no caso dos que querem comprar bitcoins, ou em bitcoins para aqueles que desejam vender a moeda digital.

Para adquirir bitcoins, o usuário fará o depósito em dinheiro e comprará as bitcoins no site da exchange. Neste momento, será necessário fazer o download de uma carteira digital para armazenar e transacionar os bitcoins, que fica armazenada no computador, telefone celular ou em dispositivo compatível. Existem vários tipos de carteiras, que geralmente se enquadram nos respectivos subgrupos.1- Carteira física ou de hardware: utiliza algum tipo de armazenamento físico para guardar as chaves, como por exemplo um pendrive; 2- Software de carteira: um aplicativo de computador, smartphone ou tablete que é usado para fazer transações e armazenar as chaves. 3- Serviço online de carteira: serviço disponibilizado em um site, que armazena as chaves para o usuário (armazenamento na nuvem). 4- Carteira off-line: qualquer tipo de carteira que nunca se conecta à internet. Na Figura 2, é possível visualizar o serviço online de carteira do site blockchain.info.

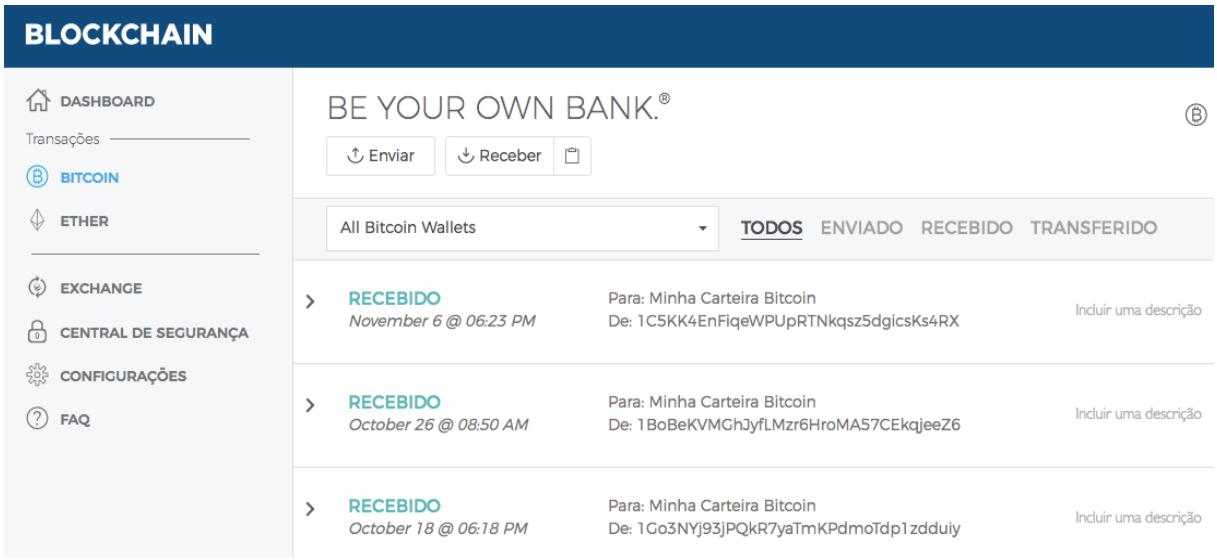

FIGURA 2: Carteira de Bitcoins.
FONTE: BLOCKCHAIN.INFO (2017).

A carteira digital cria para o usuário dois endereços formados por números e letras, chamados de chaves digitais. Uma chave é pública e outra chave é privada. A chave pública será utilizada para transacionar bitcoins com outros usuários. A chave privada serve para acessar os fundos da carteira, enquanto que a chave pública pode ser anunciada para receber fundos de outros usuários ou transferência de outras

plataformas. Vale ressaltar que, em caso de perda ou exclusão das chaves, as unidades monetárias também serão perdidas.

Uma vez criada a carteira para armazenar as bitcoins de forma segura, será necessário transferir as bitcoins adquiridas na exchange que ainda se encontram na plataforma de negociação. Normalmente, a transação ocorre em três partes: recebimento do endereço da carteira destinatária, criação da transação, onde será estabelecida a quantidade de envio, e transmissão da transação. Neste caso, está ocorrendo uma auto transferência, onde o mesmo usuário está transferindo seus bitcoins do site da exchange para o site da carteira online. Assim, será utilizada a sua chave pública da carteira para endereçar corretamente o envio das bitcoins para a carteira digital.

Vale destacar, neste momento, como funcionam as taxas de transação. Não há exigência do pagamento de taxas pelo sistema. Deste modo, os usuários opcionalmente podem pagar uma pequena taxa em cada transação. Isso fará com que a transação seja processada com maior prioridade pelos mineradores, aumentando a probabilidade de ela ser incluída mais rapidamente na blockchain. Os mineradores têm a capacidade de escolher quais transações eles irão processar, e geralmente priorizam aquelas que pagam as maiores taxas. (ALI et al, 2014).

Após sua criação, a transação será transmitida para a rede, dando início ao processo de validação das informações. Assim, ao ocorrer determinada transação, compartilha-se em rede, de modo que os demais usuários do software podem verificar a ocorrência da transação, um efeito denominado “mineração” de dados, que utiliza o poder de processamento de computadores para resolver complexos problemas matemáticos. Os “mineradores” reúnem a transação e a combinam com um novo bloco de dados do sistema. A validação consiste na confirmação de que as assinaturas estão corretas. Se a transação for válida, será adicionada a algum bloco que esteja sendo minerado no momento. Normalmente, em alguns minutos a transação será incorporada no blockchain. (ULRICH, 2014).

Finalmente, com a confirmação da transação, as bitcoins que estavam no site da exchange passam para o site da carteira online, ficando a disposição para novas transações ou para armazenamento.

2.2 Mineração e Criação da Oferta Monetária

A mineração de bitcoin é um processo pelo qual as transações são verificadas e adicionadas ao livro-razão do sistema, conhecido como blockchain, e também o meio através do qual novas bitcoins são criadas. Qualquer pessoa com acesso à Internet e hardware adequado pode participar da mineração. O processo de mineração envolve a compilação de transações recentes em blocos e a tentativa de resolver um enigma computacional de grande nível de dificuldade. O participante que primeiro resolve o quebra-cabeça coloca o próximo bloco na cadeia de blocos e reivindica as recompensas. As recompensas, que incentivam a mineração, são tanto as taxas de transação associadas às transações compiladas no bloco como as bitcoins recém criadas. O que torna a rede segura e processa as informações são os mineradores, sem os quais seria inviável a existência da bitcoin, vulnerável aos ataques. No entanto, na troca desses serviços os mineradores são compensados com bitcoins nas taxas de suas transações, pois toda vez que um minerador soluciona um algoritmo, “mina” um bloco, ao proceder desta forma será recompensado pelo block reward, com uma quantidade de bitcoins predefinida pela rede. Os bitcoins incluídos no block reward são bitcoins novos, sendo essa a forma única de os bitcoins serem criados (ULRICH, 2014).

Com relação ao número de bitcoins criados, o block reward foi designado para começar sua recompensa com 50 bitcoins por bloco adicionado à cadeia, caindo pela metade a cada 210.000 blocos criados, o que significa que para cada bloco incluído até 210.000 blocos os mineradores receberão 50 bitcoins por bloco e o próximo bloco (210.001) receberá uma recompensa de somente 25 bitcoins e assim sucessivamente. O tempo para adicionar um bloco é de cerca de 10 minutos, o que faz com que a recompensa caia pela metade aproximadamente a cada 4 anos A recompensa de bloco começou em 50 em 2009, é agora 25 em 2014, e continuará a diminuir. Essa redução de decrescente resultará em uma liberação total de bitcoins que se aproxima de 21 milhões de unidades, por volta do ano 2040. (DRAUPNIR, 2016).

No gráfico 3, temos a representação de como a Bitcoin evolui no tempo. Na linha azul, temos a projeção da base monetária da bitcoin. E na linha vermelha, a taxa de inflação (anual). Na abcissa superior, os anos; e na inferior, o número de blocos encontrados. Com a recompensa caindo pela metade a cada 210.000 blocos

adicionados, o incentivo pela mineração tonar-se menor, o que levará a um ponto onde não haverá viabilidade de se criar novas bitcoins. Isso acontece por dois motivos: primeiro, porque o número de novos mineradores no mercado tem aumentado dia após dia, isto faz com que a chance de se adicionar um bloco seja menor. Em segundo lugar, com o block reward caindo pela metade a cada 210.000 blocos adicionados, o que torna o mercado mais competitivo e menos lucrativo. (DRAUPNIR, 2016).

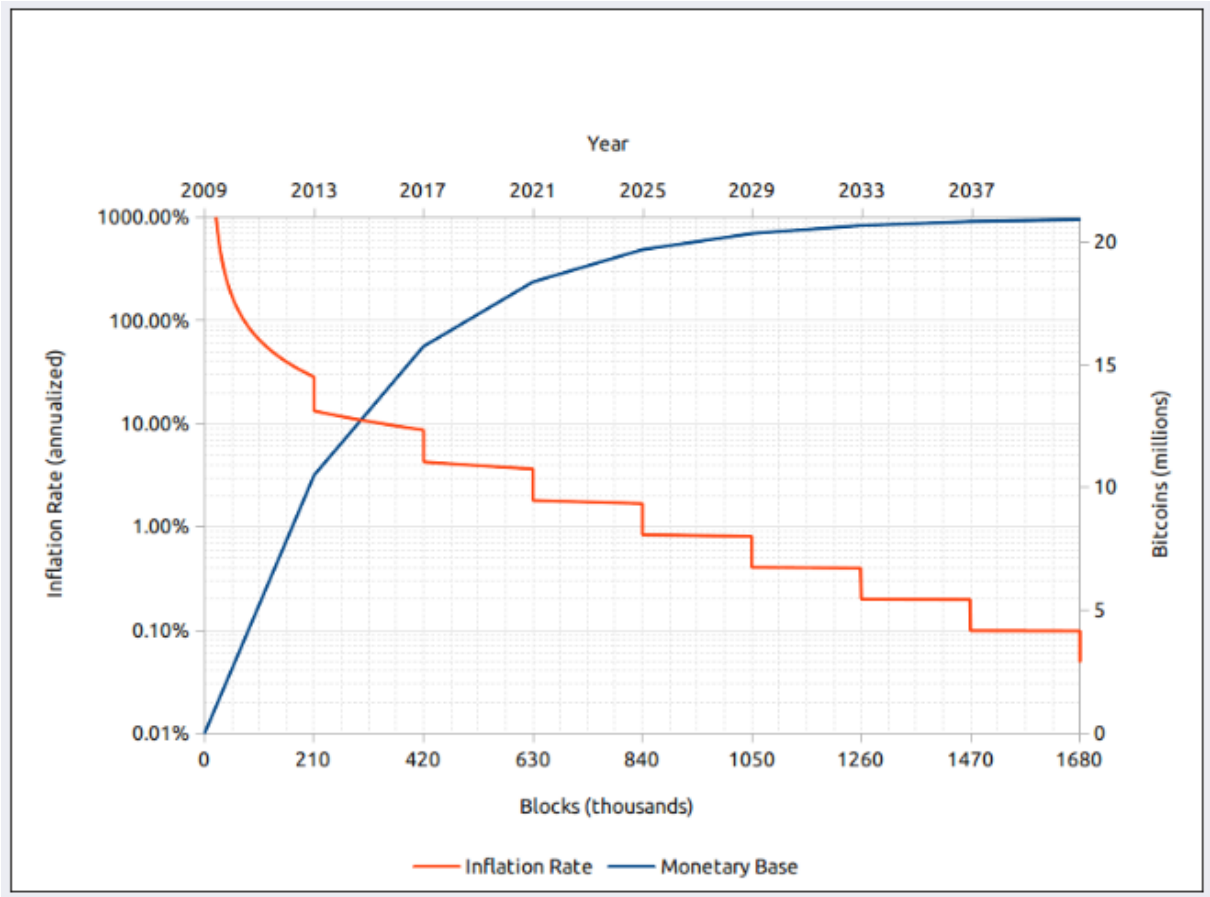

GRÁFICO 3: Inflação do Bitcoin vs. tempo.
FONTE: Draupnir (2016).

Deste modo, acredita-se que a tendência é que a bitcoin atinja maior equilíbrio e menor flutuação no valor unitário, em longo prazo, onde a base monetária estará quase no limite máximo, o mercado de mineração estará próximo ao mercado competitivo e as especulações surtirão um menor efeito sobre o preço da moeda.

A mineração cresceu a partir de um passatempo simples realizado inicialmente por usuários em computadores comuns para uma indústria de capital intensivo, que usa equipamentos de hardware personalizados e possui uma cadeia

de valor especializada (Figura 3), que pode ser resumida em cinco categorias: **Mineração**, indivíduos e organizações que utilizam seus próprios equipamentos de mineração para processar transações e ganhar a recompensa de mineração e taxas de transação; **Associações de mineração**, combina recursos computacionais de múltiplos mineradores para aumentar a probabilidade e a freqüência de encontrar um novo bloco e, em seguida, distribui recompensas de mineração entre os mineradores participantes com base na proporção de recursos computacionais contribuídos; **Fabricação de hardware de mineração,** organizações que projetam e criam equipamentos de mineração especializados; **Serviços de mineração em nuvem,** organizações que alugam o poder de mineração aos clientes; **Serviços de hospedagem remota,** organizações que hospedam e mantêm equipamento de mineração de propriedade do cliente. (HILEMAN e RAUCHS, 2017).

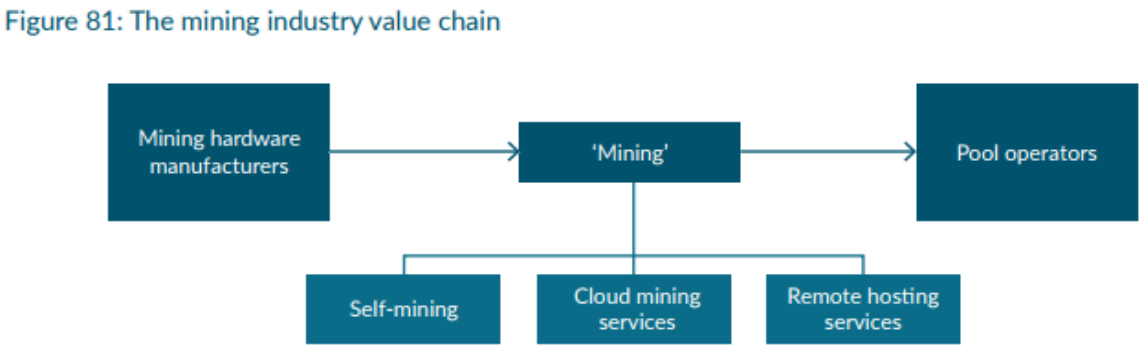

FIGURA 3: A cadeia de valor da indústria de mineração.
FONTE: Hileman e Rauchs (2017, p. 16).

Na Figura 4, a foto da mineradora Genesis Mining, empresa fundada em 2014, com sede em Hong Kong, uma das principais mineradoras de Bitcoin do mundo, além de minerar bitcoin, comercializa contratos de mineração na nuvem para investidores online, uma entre as diversas mineradoras de criptomoedas. Atualmente, as corretoras online de criptomoedas chegam a negociar compra-venda de cerca de 700 diferentes moedas digitais criptografadas, o que demonstra que existe um abrangente mercado de mineração ao redor do mundo.

FIGURA 4: Mineradora Genesis Mining.
FONTE: http://www.coinjournal.net/wp-content/uploads/2014/12/kncminer28nmimage.jpg (2014).

O custo da mineração é, basicamente, poder de processamento computacional. Na prática, isto é: hardware, energia e tempo. Vale ressaltar, a mão-de-obra necessária para a manutenção das grandes mineradoras é mínima. Geralmente, uma ou duas pessoas são suficientes para cuidar da manutenção de um “farm/mining” de grande porte. (BLOCKGEEKS ,2016).

A determinação do local geográfico de instalação de uma mineradora de criptomoedas, geralmente é baseada em três fatores-chave: os mineradores precisam ter acesso a eletricidade de baixo custo para executar suas operações de forma rentável, eles precisam ter uma conexão de internet suficientemente rápida para receber e transmitir sem atraso os dados com outros nós da rede, e os equipamentos de mineração devem ser mantidos protegidos de superaquecimento para funcionar de forma otimizada, razão pela qual os locais de baixa temperatura oferecem vantagens substanciais, pois os custos de refrigeração podem ser reduzidos. (HILEMAN e RAUCHS, 2017).

Dessa forma, as instalações de mineração são concentradas em locais onde a maioria dos fatores citados acima são satisfeitos. Estas empresas estão localizadas principalmente na América do Norte, parte Norte e Leste da Europa, e também na China. Na verdade, a China é o país que hospeda a maioria das instalações de mineração do mundo, bem como o que mais gasta energia elétrica na mineração de criptomoedas. A análise do país mostra que as instalações de mineração estão concentradas em áreas remotas, onde a eletricidade e a terra são muito baratas. Uma concentração significativa é observada na província de Sichuan, onde os mineiros tem

acordos com as usinas hidrelétricas locais para o fornecimento de energia elétrica barata. (HILEMAN e RAUCHS, 2017).

2.3 Legitimidade através da Prova de trabalho (Proof-of-work)

Outro importante ponto a ser destacado durante o processo de mineração é a forma utilizada pelo sistema para previnir ataques cibernéticos e garantir que a rede seja segura. O mecanismo é chamado prova de trabalho ou proof-of-work, em inglês. É um protocolo estabelecido para que o usuário da rede, ao executar a ação de verificação das transações, seja capaz de provar que realizou a tarefa matemática de forma completa, essa prova é a garantia de que o usuário gastou tempo para gerar a resposta que satisfaz os requesitos de validação do sistema. Para o sistema funcionar, a prova deve ser trabalhosa para ser criada, mas deve ser facilmente verificada pelo sistema de avaliação da rede. (BITCOINMINING, 2015).

Produzir uma prova de traballho pode ser um processo aleatório com baixa probabilidade, de modo que uma grande quantidade de testes e erros são necessários, em média, antes que uma prova de trabalho válida seja gerada.

No software bitcoin, as provas de trabalho são do tipo *hashcash*, e são usadas para a geração de novos blocos no blockchain. As provas de trabalho, que deverão estar incluídas nos dados de cada bloco, são necessárias para que os blocos sejam aceitas. A dificuldade deste trabalho é ajustada de modo a limitar a taxa em que novos blocos podem ser gerados pela rede em um bloco a cada 10 minutos. (BITCOINMINING, 2015).

Devido à baixíssima probabilidade de geração bem sucedida, é difícil de prever qual computador da rede será capaz de gerar o próximo bloco. Para que um bloco seja válido, ele deve indicar nos seus dados o trabalho utilizado para sua geração. Assim, cada bloco possui uma cadeia de blocos que, em conjunto, contêm uma grande quantidade de trabalho. Alterar um bloco, o que só pode ser feito fazendo um novo bloco contendo o mesmo antecessor, requer regenerar todos os sucessores e refazer o trabalho que eles contêm. Isto protege a rede blockchain contra aulteração. (BITCOINMINING, 2015).

2.4 Abrangência de Mercado do Bitcoin

De acordo com Guia do bitcoin (2017), a tecnologia blockchain traz enorme potencial para otimizar a compensação, liquidação e armazenar a poupança global, um mercado que acumula em torno de US$ 6 bilhões/ano. No mês de junho de 2017, a capitalização da criptomoeda foi em torno de 94 bilhões de dólares, e chegou a ser até maior que renomadas startups como Uber ($ 68B), Airbnb ($ 31B) e outras. E seguindo a tendência poderá ultrapassar a capitalização de mercado de grandes empresas como Starbucks ($ 94.7B), McDonalds ($ 125B) e MasterCard ($ 134B).

Atualmente, de acordo com o site blockchain.info (2017), existem cerca de 16,7 bilhões de bitcoins em circulação e o preço de mercado de 1 unidade da moeda chegou a cerca de US$ 8.000,00 em novembro de 2017 (Gráfico 4).

GRÁFICO 4: Preço de Mercado do Bitcoin.
FONTE: Blockchain.info (2017).

3 TECNOLOGIA BLOCKCHAIN: O QUE É E COMO FUNCIONA

A tecnologia blockchain se caracteriza como um banco de dados distribuído (*Distributed Ledger,* explicação na Figura 5), digital, aberto, criptografado e virtualmente disponível, trata-se de uma tecnologia que permite, por meio da matemática, concordar dados e transações sem intermediários. Nesse sentido, um

banco de dados distribuído significa um banco de dados que armazena o registro de transações invioláveis. Segundo a coin.BR.net (2017, p. 8): “a blockchain é a grande revolução tecnológica que faz do bitcoin ser uma tecnologia única e disruptiva”. Ao permitir que a informação digital seja distribuída, e não apenas copiada, a tecnologia blockchain criou os alicerces para um novo tipo de internet. Originalmente concebido para a moeda digital bitcoin, a comunidade tecnológica está agora encontrando outros usos potenciais para a tecnologia. (BLOCKGEEKS, 2016).

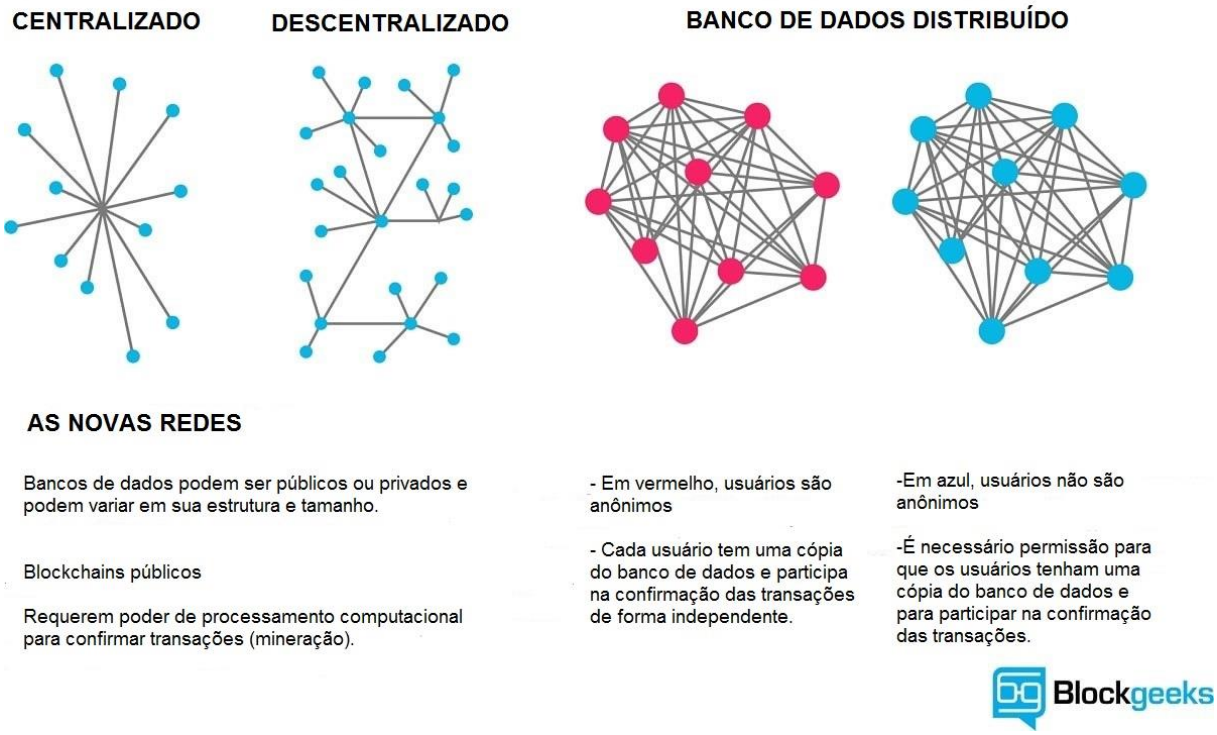

FIGURA 5: Tecnologia de Banco de Dados Distribuído.
FONTE: blockgeeks.com (2016).

Do lado esquerdo da Figura 5, pode-se observar a diferença de uma rede centralizada para uma rede descentralizada. Do lado direito, apresenta-se a ilustração da tecnologia de banco de dados distribuído, mais conhecido como blockchain. Na cor vermelha, ilustra-se uma rede de usuários anônimos, onde cada usuário tem uma cópia do banco de dados e participa na confirmação das transações de forma independente. Na cor azul, ilustra-se uma rede de usuários não anônimos, onde é requerido permissão para ter uma cópia do banco de dados e participar na confirmação das transações.

O blockchain pode ser público ou privado, variando sua estrutura e tamanho. No caso dos blockchains públicos deverá haver poder de processamento

computacional dos usuários da rede para confirmar as transações, conhecido como “mining” ou mineração, em português.

Segundo Ulrich (2014), para compreender o funcionamento do bitcoin, deve-se visualizar uma tabela duplicada milhares de vezes em uma rede de computadores projetada para ser atualizada regularmente. Assim é que funciona o blockchain, pois para cada informação armazenada em cada bloco haverá uma base de dados comum, conferida constantemente. Isso trará muitos benefícios, uma vez que o banco de dados da blockchain não é armazenado em local único, mantendo os registros públicos e de fácil verificação, não havendo uma informação com versão centralizada. Esse fato impede da informação ser danificada por hacker, sendo as cópias mantidas em milhões de computadores simultaneamente, permanecendo os dados disponíveis para todos na internet. (ULRICH, 2014).

Em uma blockchain, as transações são registradas cronologicamente, formando uma cadeia imutável e podem ser mais ou menos privadas ou anônimas dependendo de como a tecnologia é implementada. O livro-razão é distribuído por muitos participantes na rede - não existe em um só lugar. Em vez disso, as cópias existem e são atualizadas simultaneamente com cada nó (definição de nó computacional no próximo parágrafo) participante do sistema. Um bloco pode representar transações e dados de muitos tipos - moeda, direitos digitais, propriedade intelectual, identidade, títulos de propriedade, trabalho, votos, ações ou qualquer coisa que represente algum valor. A rede verifica e concorda com a transação, uma vez que cada usuário da rede tem um cópia criptografada do registro geral. Desse modo, quando alguém tenta alterar um valor, a rede simplesmente o rejeitará, por não ter consenso dos usuários que estão verificando a transação. (CATALINI, 2017).

Um nó computacional é um computador conectado a rede de computadores do blockchain por um usuário da rede, onde se verifica e transmite transações. Ele também faz o download automaticamente da cópia do bloco quando conectado a rede. Com o objetivo de incluir a transação no banco de dados primeiro que os outros, e ganhar o incentivo por ter feito primeiro, cada um desses nós executa uma série de operações matemáticas simultaneamente para validar as transações com sucesso. (BLOCKGEEKS ,2016).

A essência disruptiva do blockchain está no fato de que sempre que ocorre uma transação, existe um intermediário que a válida. Em pagamentos, isto é, por exemplo, um banco. O blockchain surge para substituir o intermediário por uma rede

de computadores (peer-to-peer), acelerando o tempo de liquidação das transações, reduzindo custos e, assim, otimizando o processo. Os principais benefícios da blockchain são: agilidade, custo, transparência e rastreamento. (BLOCKGEEKS ,2016).

Vale também ressaltar que o blockchain é uma rede que se autorregula. Para verificar as transações, equações matemáticas são solucionadas em troca de recompensas estabelecidas pela rede que utilizará o blockchain para executar suas tarefas.

3.1 Processo Operacional do Blockchain

Cada etapa de uma transação gera um conjunto de dados. Dentro do blockchain, essas transações serão agrupadas em formas de bloco. À medida que as transações vão sendo realizadas, mais blocos são adicionados, formando uma cadeia, daí surge o nome blockchain, ou blocos em cadeia, no português.

Para os blocos serem formados, é necessário que algumas regras sejam respeitadas. São elas: um tamanho máximo de transações que um bloco pode comportar e conter apenas transações que sejam verificadas como válidas – onde as duas partes envolvidas tenham aceitado a troca.

A transação entre as partes ocorre em três etapas. Pimeira etapa, criptografia: a transação é adicionada no banco de dados online e criptografado com um código digital. Segunda etapa, validação: o código da transação é enviado para a grande rede, onde a autenticidade do código é confirmada sem o comprometimento da informações privada. E também, eliminando a necessidade de uma autoridade central presente para validar a transação. Terceira etapa, distribuição: uma vez que a transação é confirmada e validada por muitos nós da rede, ela passa a existir no banco de dados de cada um destes nós, como um registro permanente e imutável da transação; a informação da transação é gravada no banco de dados público da rede, e a transação é concluída.

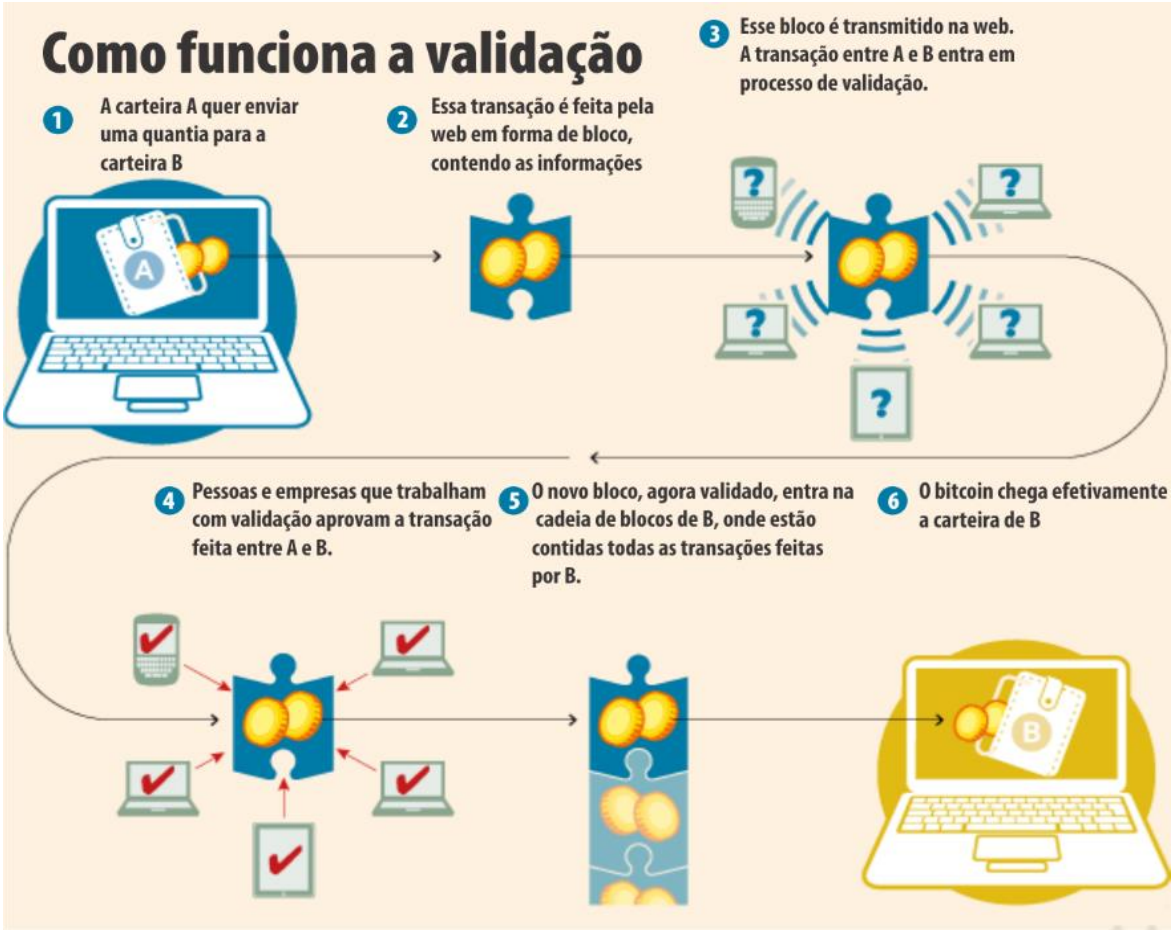

FIGURA 2: Processo do blockchain.
FONTE: http://amandaliraduarte.com/blockchain/ (2017)

3.2 Redução de Custos com o Blockchain

Existem dois tipos de custos que o blockchain é capaz de reduzir no mercado: custo de verificação e o custo de rede.

Cada empresa e organização se envolve em vários tipos de transações todos os dias. Cada uma dessas transações requer verificação. Em muitos casos, essa verificação é fácil. As empresas conhecem seus clientes, seus colegas e seus parceiros de negócios. Tendo trabalhado com eles e seus produtos, dados ou informações, você tem uma boa idéia de seu valor e confiabilidade. Entretanto, segundo Catalini (2017), quando surge um problema, muitas vezes temos que realizar algum tipo de confirmação ou aditoria. Em muitos casos, é necessária a execução de algum processo para se certificar de que a pessoa que reivindica ter determinadas credenciais realmente tem tais credenciais, ou se a empresa que está vendendo os produtos possui, de fato, a certificação que afirma ter. Quando estes processos são

necessários, torna-se custoso e intensivo em mão-de-obra para as empresas. (CATALINI, 2017).

A razão pela qual os bancos de dados distribuídos são tão úteis nesses casos é porque, se esses dados ou atributos foram gravados blockchain, e torna-se necessária a verificação da autenticidade de alguma credencial, por exemplo, pode-se sempre voltar no bloco desejado e encaminhá-los sem nenhum custo. É uma verificação sem custo. Desse modo, pode-se entender a enorme funcionalidade do bitcoin, dado que ele pode verificar de forma econômica que os fundos estão realmente lá. Pode-se transferir o valor para qualquer lugar do globo em custo de transação quase zero. Enviar mensagens seguras que carregam valor não requer mais um banco ou PayPal no meio. Em resumo, como o blockchain verifica a confiabilidade, ninguém mais precisa verificar, e o atrito da transação é reduzido, o que resulta em economia de custos e de tempo. (CATALINI, 2017).

Utilizar o blockchain também pode reduzir o custo de executar uma rede segura. A blockchain possibilita a criação de novos tipos de plataformas onde a troca e a provisão de ativos digitais não dependen de um intermediário. Nessas plataformas, a confiança de um operador de plataforma é substituída pela confiança nos códigos, incentivos subjacentes e consenso de regras do sistema. Como resultado, o poder de mercado do intermediário, o risco de privacidade, e o risco de censura são drasticamente reduzidos. (CATALINI e GANS, 2017).

A tecnologia blockchain, ao reduzir significantemente o custo de execução de redes descentralizadas de troca, permite a criação de plataformas digitais onde os benefícios da rede e da infra-estrutura digital compartilhada não vem ao custo do aumento do poder de mercado e acesso de dados por um intermediário. Essa redução no custo da rede gera profundas consequências para a estrutura do mercado, pois permite a startups e projetos de código aberto a competição direta com os players vigentes no mercado. Isto ocorre através de um novo design das plataformas onde os efeitos diretos e indiretos da rede são amplamente compartilhados entre os participantes (desenvolvedores, usuários, investidores), e nenhum player tem total controle sobre os ativos digitais e os dados. (CATALINI e GANS, 2017).

Além disso, devido a ausência de uma “câmara de compensação” centralizada, essa novas plataformas permitem que sejam executadas inovações sem permissão. Desde que a aplicação seja compatível com o protocolo estabelecido e com as regras de consenso, as implementações na rede podem ser impantadas sem a permissão de

outros participantes. Desse modo, uma vez que cada colaborador de uma plataforma baseada em blockchain pode moldar sua evolução, de modo proporcional a sua participação (em termos de poder de processamento, armazenamento, trabalho ou capital dedicado), essas plataformas podem democraticamente desenvolver-se ao longo do tempo para acomodar mudanças na organização do mercado que beneficiem a maioria dos colaboradores. (CATALINI e GANS, 2017).

3.3 Segurança na Nova Rede

Uma vez que os dados estão espelhados por toda a rede, o sistema de blockchain é muito mais seguro do que os sistemas que armazenam dados de forma centralizada. Desse modo, a rede blockchain não tem pontos de vulnerabilidade, que poderiam ser utilizados por hackers, por exemplo. (BLOCKGEEKS ,2016).

Alterar uma transação no blockchain não é tão simples quanto pode parecer em um primeiro momento. Alterar um dado em uma rede distribuída significa ter que “enganar” toda a a rede, isso sem contar a parte de criptografia que para ser quebrada exigiria enorme poder de processamento computacional, tempo e energia. Para realizar a uma alteração no sistema, o hacker teria que encontrar o bloco certo, descriptografas (tarefa quase impossível) e encontrar a transação para ser alterada. Após alterar a transação, e por consequência, também o bloco, seria gerado um novo blockchain diferente do que está na rede. Ou seja, não basta simplismente recolocar o bloco na rede, pois a rede reconheceria aquele novo blockchain como inválido, uma vez que é diferente do blockchain já autenticado. Então, seria necessário reescrever todos os blocos anteriores para que a adulteração fosse aceita. Para isso, seria necessário mais que 50% da potência computacional de toda a rede dedicada por muito tempo, gerando um custo altíssimo. Enquanto isso, outros nós da já rejeitariam a alteração, o que torna praticamente impossível corromper a rede.

Sem contar que, hoje em dia, normalmente confia-se em sistemas que utilizam “nome de usuário e senha” para proteger identidade e ativos online. No blockchain, os métodos de segurança utilizam tecnologia de criptografia, baseando-se nas chamadas chaves públicas e privadas, para garantir que somente participantes envolvidos em uma transação visualizarão a informação. A chave pública (uma série longa de números gerados aleatoriamente) é o endereço do usuário no bloco. No caso do bitcoin, quando valores são enviados para um usuário, o registro gravará a

transação como pertencentes a esse endereço (chave pública do usuário). A chave privada é uma senha que dá ao proprietário acesso a seus bitcoins. A seguir, apresento a chave pública de minha carteira de bitcoins pessoal, para exemplificar seu formato: 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v. (BLOCKGEEKS ,2016).

4 POSSIBILIDADES DE APLICAÇÃO DO BLOCKCHAIN

Na próxima sessão, apresento algumas das possibilidades de aplicação da tecnologia apresentada. Especialistas classificam o blockchain como uma tecnologia de propósito geral, e afirmam que nos próximos anos veremos sua aplicação em diferentes setores e ramos de atuação.

Até mesmo bancos centrais, entre eles o do Canadá, Cingapura e Inglaterra, estão estudando e experimentando a tecnologia blockchain e as criptomoedas. As aplicações potenciais incluem menor risco de liquidação, tributação mais eficiente, pagamentos transfronteiriços mais rápidos e pagamentos interbancários. (CATALINI, 2017).

4.1 Serviços Financeiros

Os sistemas financeiros tradicionais tendem a ser incomodos, propensos a erros e lentos. Intermediários são freqüentemente necessários para mediar os processos e resolver conflitos. Naturalmente, isso gera custos em estresse, tempo e dinheiro. Em contraste, surge o blockchain, um sistema mais barato, mais transparente e mais eficaz. Não é de admirar que um número crescente de serviços financeiros esteja usando esse sistema para introduzir inovações, como títulos inteligentes e contratos inteligentes. O primeiro paga automaticamente os títulos aos seus proprietários assim que determinados termos pré-programados são atendidos. Estes últimos são contratos digitais que se auto-executam e auto-mantêm, novamente quando os termos são atendidos. A seguir alguns exemplos de aplicação do blockchain para serviços financeiros.

Gestão de ativos: os processos de comércio tradicional, onde as partes negociam e gerenciam ativos, podem ser caros e arriscandos, principalmente quando se trata de transações entre fronteiras. Cada parte do processo, como o corretor, o custodiante, ou o gerente de liquidação, mantêm seus próprios registros, o que cria

ineficiências significativas e espaço para erros. O blockchain reduz o erro criptografando os registros, ao mesmo tempo que simplifica o processo, cancelando a necessidade de intermediários. Ações de empresas também podem ser negociadas por meio da tecnologia blockchain. Isso possibilitaria uma melhoria em toda a estrutra, na medida em que poderia trazer o histórico completo de cada ação e reduzir drasticamente a burocracia e papel impresso. Pode-se imaginar como as corretoras usarão esta tecnologia. Ao reduzir as partes intermediárias os custos de corretagem também se reduzirão, e ao mesmo tempo tornarão as transações mais seguras e transparentes. (BLOCKGEEKS ,2016).

Seguros: o processamento de sinistros pode ser um procedimento frustrante e ingrato. Os processadores de seguros devem lidar com reinvindicações fraudulentas, fontes de dados fragmentadas e processam esses formulários manualmente, dando enorme espaço para o erro. O blockchain fornece um sistema perfeito para gerenciamento e transparência, livre de riscos. (BLOCKGEEKS ,2016).

Pagamentos internacionais: setor de pagamentos globais é propenso a erros, dispendioso e sujeito a lavagem de dinheiro. Pode chegar a demorar dias para o dinheiro atravessar o mundo. O blockchain já está fornecendo soluções em empresas de remessas internacionais, como Abra, Align Commerce e Bitspark que oferecem serviços de remessa baseados em blockchain, de ponta a ponta. Em 2014, o Santander tornou-se um dos primeiros bancos a fundir o blockchain a um aplicativo de pagamentos, permitindo que os clientes efetuassem pagamentos internacionais, 24 horas por dia, com liquidação para o dia seguinte. (BLOCKGEEKS ,2016).

4.2 Propriedades Inteligentes

Atualmente alguns papéis registrados em cartório e valores em alguns bancos de dados confirmam a propriedade de uma pessoa sobre um bem imóvel, por exemplo. Nesse processo, pode-se pensar, ainda, em outras pessoas envolvidas em cada etapa do trâmite e despesas geradas para conseguir cada papel assinado.

Uma propriedade pode ser tangível, como carros, casas ou mobiliário doméstico, ou intangível, como patentes, títulos de propriedade ou ações de uma empresa. Esse registro pode ser armazenado no blockchain, juntamente com detalhes contratuais de outras pessoas que também têm o direito de propriedade sobre tais bens. Chaves inteligentes podem ser usadas para facilitar o acesso à propriedade. O

banco de dados distribuído também se torna um sistema para registrar e gerenciar direitos de propriedade, além de permitir que os contratos inteligentes sejam duplicados se os registros ou as chaves inteligentes forem perdidos. Trabalhar com propriedades inteligentes diminui os riscos de se deparar com fraude, taxas de mediação e situações de negócios questionáveis. Ao mesmo tempo, aumenta a confiança e a eficiência. (BLOCKGEEKS ,2016).

4.3 Contratos Inteligentes

Contratos inteligentes são contratos digitais que estão incorporados com um código de processamento condicional, por exemplo: se o parâmetro x for atingido, então y será acionado, em um sistema que lhes permite execução automática. Em um contrato convencional, um intermediário garante que todas as partes sigam os termos pré-estabelecidos. O blockchain renuncia a necessidade de terceiros, e também garante que todos os participantes conheçam os detalhes do contrato. Além disso, implementa os termos contratuais automaticamente quando as condições são atendidas. Contratos inteligentes podem ser utilizados para todos os tipos de situação, tais como derivativos financeiros, prêmios de seguros, leis de propriedade, acordos de crowdfunding e internet das coisas (IOT). Os contratos inteligentes permitem a automatização do gerenciamento remoto de sistemas, no caso da internet das coisas (IOT). A combinação de software, sensores e rede facilita a troca de dados entre objetos e mecanismos. Nesse sentido, a eficiência do sistema é otimizada e o controle de custos é melhorado.(BLOCKGEEKS ,2016).

4.4 Governança

Bancos de dados distribuídos também tem utilidade para decisões organizacionais. A gestão de ativos, capital ou informação feitas pelo administrativo das empresas e governamentais tornam-se completamente transparentes e verificáveis. Torna-se possível verificar se as declarações éticas das empresas a respeitos de seus produtos e matérias-primas são verdadeiras. O blockchain permite que a história das coisas que compramos seja genuína, fornecendo informações a respeito da data, local e marcas. Poderá servir, por exemplo, para regulamentar o mercado de diamantes e demais bens passíveis de contrabando e mercado negro.

Com a blockchain, no futuro, poderemos ter a transparência total das eleições ou qualquer outro tipo de pesquisa de opinião, pois tonar os resultados totalmente transparentes e acessíveis ao público. Os votos podem ser registrados e enviados (da pessoa que detém o voto, para um candidato, ideia, partido ou projeto de lei) através de um aplicativo que usa blockchain, tornando-se menos vulnerável às falhas técnicas e melhor protegido contra adulterações. (BLOCKGEEKS ,2016).

CONCLUSÃO

A tecnologia blockchain vem revolucionando o setor financeiro, mas a própria internet está sendo remodelada, e também a noção de rede, desde o usuário até os governos e as grandes corporações. Logo, o tema será matéria obrigatória nas áreas de TI, e passaremos a ouvir cada vez mais sobre o assunto. Com esperança, a tecnologia encontrará bom uso para o progresso da humanidade, e para a qualidade de vida das pessoas, tornando a sociedade mais justa e transparente. Vale ressaltar a importância do aprofundamento do estudo acerca da Blockchain, para que os possíveis malefícios trazidos pela tecnologia possam ser contornados e combatidos.

Já sobre a bitcoin, o futuro é bastante incerto, porém sua participação no mercado é cada vez mais significativa. O mercado de moedas digitais, como um todo, veio para ficar e novas alternativas vêm surgindo e crescendo todos os dias. Existe demanda real por esses itens. Atualmente, os casos de uso mais bem sucedidos ajudam aqueles que são desbancarizados, ou os que precisam enviar dinheiro de um país a outro, sem contar com a possibilidade de realizar micropagamentos de forma segura, transparente e de baixo custo. Em países onde existe hiperinflação, a moeda tem se mostrado uma excelente forma de reserva de valor, protegendo os usuários de governos muitas vezes ineficientes e ditatorias, como vem acontecendo na Venezuela, por exemplo.

Nota-se, ainda, que há muita especulação e discussões legais sobre as criptomoedas. Há, também, muito oportunismo em torno da bitcoin, especialmente por conta da valorização e volatilidade que ocorrem nessa fase inicial da moeda. Com certeza, o novo sistema pode ser encarado como o futuro dos meios de pagamento para o comércio eletrônico, porém, muitos ainda a consideram apenas como mais um ativo volátil que está submetido a especulação financeira. Nesse sentido, pode-se encarar o bitcoin como o precursor de um longo caminho que as moedas digitais percorrerão até que seja alcançado o ideal monetário, mas, desde já, contribuindo para melhorias no sistema financeiro vigente. Além disso, impulsiona a discussão da centralização, regulamentação e distribuição monetária, tal como ocorre nos dias atuais, tendo como foco as crises, inflações e participação das instituições financeiras.

Apesar da grande notoriedade, a bitcoin não tomará o lugar das moedas nacionais em nenhum momento próximo, e parece não ter motivo para tal. A sua verdadeira popularidade é por funcionar como uma alternativa à moeda nacional. Hoje

em dia, a grande procura pela bitcoin ainda reside na expectativa de rentabilidade futura, como um ativo financeiro e não em seu uso como meio de troca, o qual ainda é fraco, tornando a moeda presa ao dinheiro nacional para o consumo de mercadorias. O sentimento sobre o bitcoin mais presente na mídia é a exaltação pela valorização do ativo virtual. A cada nova marca histórica alcançada pela moeda, a empolgação é visível e em momentos de quedas abruptas nos preços o alarmismo se instala.

Desse modo, o abandono das moedas nacionais em troca de um sistema monetário totalmente descentralizado é uma utopia distante. A questão mais relevante é qual será o impacto que um sistema de transações descentralizado poderá ocasionar no sistema bancário e financeiro atual, ao possibilitar transações mais rápidas, de custo reduzido, seguras, e mais eficientes. É certo que as bitcoins continuarão se desenvolvendo como uma moeda paralela à nacional, mas o impacto do seu crescimento ainda dependerá do grau de utilização que a mesma poderá adquirir no decorrer do tempo. O que poderá acontecer com o sistema bancário quando este conhecimento se tornar disseminado e as pessoas optarem pelos benefícios das transações descentralizadas continua sendo uma dúvida.

.

REFERÊNCIAS

17 Blockchains Applications That Are Transforming Society. BlockGeeks. 2016. Disponível em:< https://blockgeeks.com/guides/blockchain-applications/> Acesso em: 14 nov 2017.

ALI, Robleh et al. Innovations in payment technologies and the emergence of digital currencies. Quarterly Bulletin, Bank of England, London, 2014. Disponível em: <http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf> Acesso em: 10 out 2017.

BANCO CENTRAL DO BRASIL (BACEN). Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais. Brasília, 2017. Disponível em:<http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017> Acesso em: 14 Nov 2017.

CATALINI, Christian. Blockchain, explained. An MIT expert on why distributed ledgers and cryptocurrencies have the potential to affect every industry. MIT Management Sloan School. 2017. Disponível em: http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/. Acesso em: 14 nov 2017.

CATALINI, Christian; GANS, Joshua S. Some Simple Economics of the Blockchain. MIT and University of Toronto. 2017. Disponível em: http://blockchain.mit.edu/. Acesso em 14 nov 2017.

DRAUPNIR, Melvin. Bitcoin Mining. How are New Bitcoins Created and Generated? 2016. Disponível em: <https://www.bitcoinmining.com/how-are-new-bitcoins-created/> Acesso em: 10 out 2017.

Guia básico sobre bitcoin. coinBR.netblockchainTech. 2017. Disponível em: <https://coinbr.net/media/pdfs/btc-guide-pt.pdf>. Acesso em 9 out 2017.

HILEMAN, Garrick; RAUCHS, Michel. Global cryptocurrency benchmarking study. Universidade of Cambridge Judge Business School. Cambridge Centre Alternative Finance. 2017. Disponível em: <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf>. Acesso em 28 set 2017.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Disponível em: <http://bitcoin.org/bitcoin.pdf>. Acesso em: 15 ago 2017.

SMAAL, Beatriz. Techtudo. Bitcoin: A mineração de moedas. 2014. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2014/01/bitcoin-a-mineracao-de-moedas.html> Acesso em: 13 nov 2017.

URLICH, Fernando. Bitcoin: A moeda na era digital. 1. ed. São Paulo: Mises Brasil, 2014.

What is Blockchain technology? A Step-by-Step Guide For Beginners. BlockGeeks. 2016. Disponível em:< https://blockgeeks.com/guides/what-is-blockchain-technology/> Acesso em: 14 nov 2017.

What is Proof of Work. Bitcoin Mining. 2015. Disponível em: <https://www.bitcoinmining.com/what-is-proof-of-work/>. Acesso em: 14 nov 2017.